Security Vulnerabilities Of Scada Communication Protocols

Rajesh L, P Satyanarayana

Abstract: SCADA system plays a key role in Industrial Control Systems for monitoring and remote controlling process plants like Oil & Gas refineries, nuclear power plants, power generation and manufacturing industries. These systems are sharing sensor data to external world through internet and company corporate networks. It opens the doors for cyber security attacks. Communication protocols are running in SCADA systems for continually transferring sensor data to SCADA servers and vice-versa. MODBUS is one of the most widely used protocols in SCADA systems. In this paper, we reviewed security of SCADA systems, communication protocols and proposed methods to enhance the security of these protocols.

Index Terms: Communication Protocol, Cyber Security, Industrial Control Systems, MODBUS, PLC, RTU, SCADA Systems.

1. INTRODUCTION

The National Critical Infrastructure (NCI) facilities like Oil & Gas Refineries, Nuclear Power Plants, Manufacturing industries etc. are working using Supervisory Control and data acquisition systems (SCADA) for displaying the field data and controlling the field instruments by control commands [1]. These systems are also called Process Control Systems (PCS) or Industrial Control Systems (ICS). These systems provide automation of plants. They reduce human intervention and increase the efficiency of the plant by reducing the errors [2]. In old days, these systems were installed in a control room and there was no connectivity to internet or external world. But now-a-days, with technology progress, these systems are connected to internet for remote monitoring and sharing the SCADA data to other systems like ERP [3]. Hence these systems are vulnerable to cyber-attacks and needs to protect SCADA systems [4]. SCADA systems need to protect for safe and secure operations of process plants and Critical National Infrastructures. The security of SCADA systems is one of critical aspects of designing the system. The security measures of Information and Communication Technology (ICT) systems cannot apply for these SCADA systems because these systems are running in 24*7 continuous operation and real time systems [5]. We cannot shutdown the plants after loading a patch etc. The security measures will be different and they should create any intervention to operation of the plats [6]. Security of SCADA communication protocols is one of the important areas for security of SCADA systems [7]. In this section, we will take MODBUS as example to consider and explains the security issues of MODBUS protocol. In this paper, we explained basic components of SCADA systems in section II, literature review in section III. We proposed methods to enhance the security of SCADA systems in section IV and concluded the paper in section V.

2. SCADA SYSTEM COMPONENTS

As shown in Fig. 1, main components of SCADA systems [8]:

2.1 Field Instruments or sensors
2.2 Programmable Logic Controllers (PLCs)
2.3 IT hardware like Servers, Work Stations
2.4 Network equipment

2.1 Field Instruments or sensors

Field Instruments contains sensors to sense the signal. Example is Pressure transmitter for sensing pressure in the pipe line. These instruments collect data from field and sends to PLC or Remote Telemetry Units (RTUs). PLC will process the data and sends to SCADA Server for further processing. For example Pressure transmitter detects 50 kg/cm2 of pressure in 0-100 kg/cm2 scale. Then PT converts this value of 50 kg/cm2 to electrical signal of 4-20 mA scale. Hence it sends 12 mA to PLC.

2.2 Programmable Logic Controller (PLC)

PLC is a microprocessor with input/output cards. The sensor data will be collected by these IO cards and logic will be executed based on this data. Various interlocks will be checked and processed in PLC. PLC will send the sensor data to SCADA Server. The PLC will receive and converts 12 mA current to 8000 count value of 0-16000 scale and sends to SCADA Server.

2.3 IT Hardware

The IT hardware contains SCADA Servers, workstations, engineering stations, Historian Servers etc. These systems are collecting, processing the sensor data and displays the data in various formats. SCADA Servers polls PLC for data transfer and sends it after formatting to human readable format, like scaling with engineering units. Historian will store the data for years. Workstations or clients will display data in various formats like mimics, trends, reports etc.

- *Rajesh L is a research scholar in ECE department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, india. E-mail: locharalarajesh@gmail.com*
- *P Satyanarayana is working as Professor, in ECE department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, india. E-mail: satece@kluniversity.in*

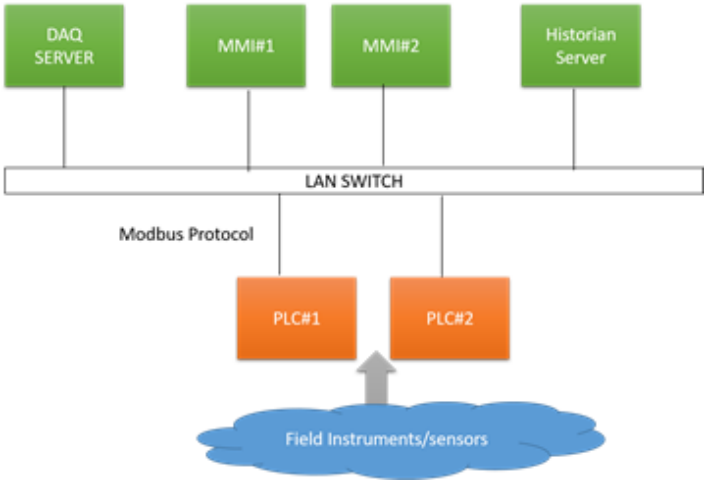

***Fig. 1**. A typical SCADA architecture*

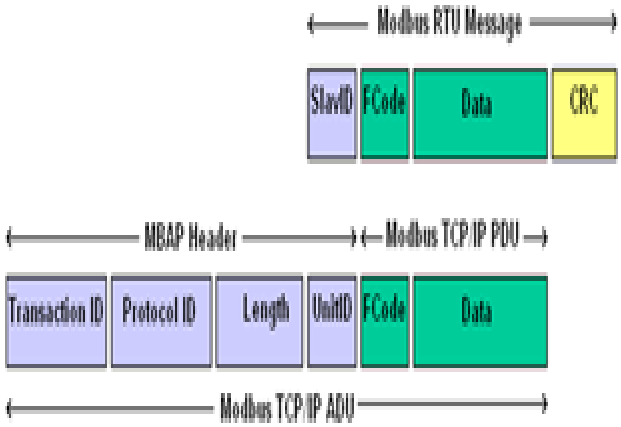

***Fig. 2**. MODBUS Frame structure [11]*

2.4 Network Equipment

SCADA systems are connected in the network using Local Area Network (LAN) using network LAN switches and WAN using routers. Various IP schemes will be defined to inter connect these systems.

2.5 Communication Protocols

SCADA systems are using various communication protocols like MODBUS, DNP, IEC 60870-1-101/104, Profinet, Profibus. EthernetIP etc for bi-directional data transfer between various nodes in network [9]. MODBUS is most widely used protocol between PLC and SCADA Servers [10]. Modbus is a simple request reply protocol. It is an application layer protocol [11]. Server will send the request and PLC will respond the request with correct response or exception response [12]. MODBUS frame packet is encapsulated on TCP/IP and it is called MODBUS TCP/IP. The MODBUS frame format is shown in Fig. 2 [13].

3. LITERATURE SURVEY

In literature, various research scholars explained the importance of security of SCADA systems, communication protocols. Some of the research persons proposed, and implemented some methods. Huitsing *et al.* [14] explained various attack scenarios in Modbus serial and TCP/IP protocols. Nardone *et al.* [15] described security issues of Modbus protocol. While designing this protocol in 70's, security was not an important issue and security measures were not considered. This protocol is more vulnerable to cyber-attacks. It suffers from the following security issues [16]: Anybody can take control of PLC because of lack of authentication. Modbus will not check IP address authentication. Due to lack of authorization, any attacker can send commands to close the running pump etc. As integrity checking is not available anybody can change the MODBUS frame in middle and send false response to server or false command to PLC. Due to non-availability of various security checks, Modbus is suffering from following attacks: Man-in-the Middle attack, false command injection, false command injection, Daniel of Service (DoS) attack [17]. Morris, T et al. [18-19] defines rules for detecting attacks in Modbus protocol but they cannot protect or prevent to occur. Fevino *et al.* [20] implemented a method where RSA, Hash functionality was implemented on Modbus frame, but the final frame is transferred in plain text. Shahzad *et al.* [21-23] proposed and implemented various methods for security enhancement of Modbus protocols but the methods change the frame formats of Modbus protocol and became proprietary protocols. They are not suitable for legacy systems and does not provide backward compatibility. Rajesh L *et al.* [24] described various possible attacks on Modbus protocol and simulated the attacks and studied the effect of these attacks on Modbus protocol. From the literature review, we concluded that SCADA systems are vulnerable to cyber security attacks and needs to protect these systems for safe and secure operation of process plants. SCADA communication protocols plays important role in execution of these systems and needs to safe guard these protocol from security attacks.

4. PROPOSED METHODS

It was understood that the existing solutions are mostly changed the Modbus frame formats and made the protocol customized and proprietary protocols. They cannot be applied to old existing legacy systems. They also not provided interoperability between various vendors manufactured systems. We proposed an open method for enhancing the security of MODBUS protocols in SCADA systems. Instead of connecting PLC and DAQ Server in SCADA network, two modules will be developed. They are called gateway1 and gateway 2. At Server side the module is called gateway1, PLC side it is called gateway2. The bi-directional data transfer between PLC and Server will take place through these gateway modules. Various cryptographic algorithms can be applied on protocol frames, in these gateway modules. Researchers can try AES, RSA, elliptic curve algorithms for confidentiality, Hash functionality to achieve integrity of the frame. Authorization of source address with filtering concept can be developed. The proposed method was explained in

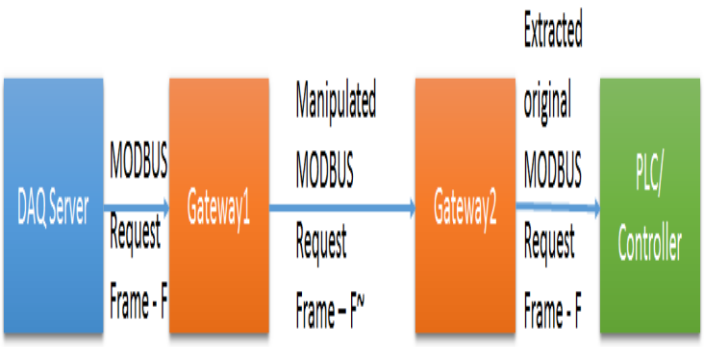

***Fig. 3**. Proposed solution with gateway modules*

block diagram as shown in Fig. 3. The advantage of this method is it can be applied to any legacy system and any SCADA system be any vendor. It provides interoperability between systems from various vendors. Time stamp of the frame can be developed to protect from replay attacks. The Table-I explains how the propose method provides security to MODBUS protocol. There are number of cryptographic algorithms available to apply on Modbus for confidentiality of frame. In addition to Hash function like SHA-512, CRC/LRC can be added to avoid errors in the frame during transmission. Two bytes of synchronization bytes can be added to take fine boundaries of frame. Various filtering schemes can be applied before sending the Modbus frame to PLC to filter the frame, if it is not supported. The flow chart of proposed scheme is shown in Fig. 4. In future we will try to implement the methods and test the total system. But the designer has to consider various performance parameters before selecting the methods. They have to estimate how much overhead will take place on Modbus frame size, calculation time, encryption decryption conversion time, scanning time, round trip time from Modbus request to response at Server. The developed methods should not increase the scan time or update time at SCADA mimics.

5. CONCLUSION

SCADA systems are monitoring and controlling process plants. These systems are vulnerable to security attacks because of connectivity to internet and corporate networks. SCADA protocols are one of areas where attention is required. In this paper we reviewed existing methods for enhancing security of SCADA protocols and proposed a new method which is suitable to existing legacy systems. In future we will develop the solution and test the system with simulation of various security attacks.

6 ACKNOWLEDGMENT

The authors wish to thank K L Deemed to be university to conduct the research.

Parameter	How it protected
Confidentiality	AES algorithm (AES-256)
Integrity	Hash (SHA-512)
Non repudiation	RSA algorithm
Authentication	IP address, user name and password checking

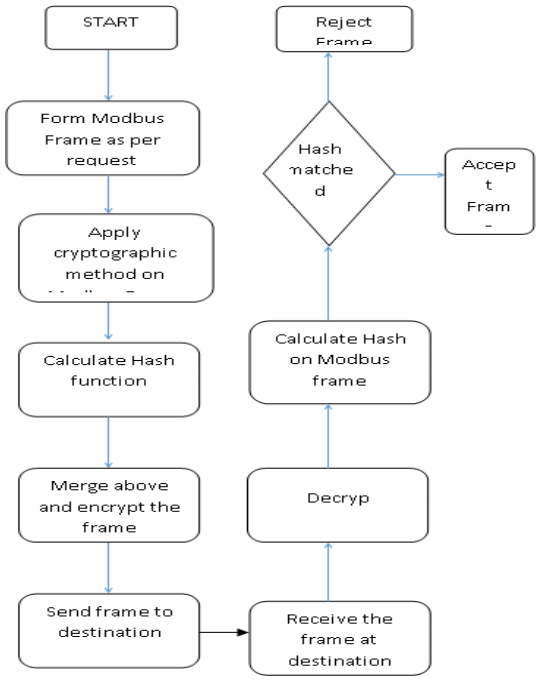

***Fig. 4**. Flow chart of proposed method*

9 REFERENCES

[1]. Jason Stamp, John Dillinger, William Young, and Jennifer DePoy." common vulnerabilities in critical infrastructure control systems" SANS SANSFIRE 2003 and National Information Assurance Leadership Conference V – (NIAL), July 14-22, 2003, Washingdon, DC

[2]. Alvaro A. C ardenas, Saurabh Amin, Shankar Sastry. "Research Challenges for the Security of Control Systems", 3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium. San Jose, CA, USA. July 2008.

[3]. https://www.dhs.gov/critical-infrastructure-sectors

[4]. https://ics-cert.us-cert.gov/

[5]. Zio, E. (2016). “Critical Infrastructures Vulnerability and Risk Analysis”, European Journal for Security Research, 1(2), 97-114. doi:10.1007/s41125-016-0004-2

[6]. Song, Jae-Gu, Jung-Woon Lee, Gee-Yong Park, Kee-Choon Kwon, Dong-Young Lee, and Cheol-Kwon Lee. "An Analysis Of Technical Security Control Requirements For Digital I&c Systems In Nuclear Power Plants." Nuclear Engineering and Technology 45.5 (2013): 637-52. Web.

[7]. Cherdantseva, Yulia, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. "A review of cyber security risk assessment methods for SCADA systems." Computers & Security 56 (2016): 1-27. Web.

[8]. Dobriceanu, Mircea, et al. "SCADA system for monitoring water supply networks." WSEAS Transactions on Systems 7.10 (2008): 1070-1079.

[9]. Graham, J.; Patel, S ., (2004), “Security Considerations In SCADA Communication Protocols.” Technical Report Tr-Isrl-04-01; Intelligent Systems Research Laboratory: Louisville, KY, USA.

[10]. Kang, Dong-Joo, Jong-Joo Lee, Seog-Joo Kim, and Jong-Hyuk Park. "Analysis on cyber threats to SCADA systems." 2009 Transmission & Distribution Conference & Exposition: Asia and Pacific (2009)
[11]. MODBUS Over Serial Line Specification & Implementation Guide V1.02, Modbus Organization, Dec 20, 2006
[12]. MODBUS Messaging On Tcp/Ip Implementation Guide V1.0b, Modbus Organization, Oct 24, 2006
[13]. MODBUS Appl Protocol Specification V1.1 b3, Modbus Organization, April 26, 2012
[14]. Huitsing, Peter, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi. "Attack taxonomies for the Modbus protocols." International Journal of Critical Infrastructure Protection 1 (2008): 37-44. doi:10.1016/j.ijcip.2008.08.003.
[15]. Nardone, Roberto, Ricardo J. Rodriguez, and Stefano Marrone. "Formal security assessment of Modbus protocol." 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (2016)
[16]. Rajesh, L., and Penke Satyanarayana. “Communication Protocol Security in Industrial Control Systems to Protect National Critical Infrastructure.” Journal of Advanced Research in Dynamical and Control Systems 9.6 (2017): 290–304
[17]. Pidikiti, D. S., Kalluri, R., Kumar, R. K., & Bindhumadhava, B. S. (2013). “SCADA communication protocols: vulnerabilities, attacks and possible mitigations”. CSI Transactions on ICT,1(2), 135-141. doi:10.1007/s40012-013-0013-5
[18]. Morris, T. H., Jones, B. A., Vaughn, R. B., & Dandass, Y. S. (2013). “Deterministic Intrusion Detection Rules for MODBUS Protocols. 2013 46th Hawaii International Conference on System Sciences”. doi:10.1109/hicss.2013.174
[19]. Morris, T., Vaughn, R., & Dandass, Y. (2012). “A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems “. 2012 45th Hawaii International Conference on System Sciences. doi:10.1109/hicss.2012.78
[20]. Fovino, I. N., Carcano, A., Masera, M., & Trombetta, A. (2009). “Design and Implementation of a Secure Modbus Protocol”. IFIP Advances in Information and Communication Technology Critical Infrastructure Protection III, 83-96. doi:10.1007/978-3-642-04798-5_6
[21]. Shahzad, A., Lee, M., Lee, Y., Kim, S., Xiong, N., Choi, J., & Cho, Y. (2015). Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information. Symmetry,7(3), 1176-1210. doi:10.3390/sym7031176
[22]. Shahzad, A., Musa, S., & Irfan, M. (2014). Security Solution for SCADA Protocols Communication during Multicasting and Polling Scenario. Trends in Applied Sciences Research,9(7), 396-405. doi:10.3923/tasr.2014.396.405
[23]. Shahzad, A.A. and S. Musa, 2012. Cryptography and authentication placement to provide secure channel for SCADA communication. International Journal of Security., 6: 28-44.
[24]. L. Rajesh, P. Satyanarayana, “Vulnerability Analysis and Enhancement of Security of Communication Protocol in Industrial Control Systems”, Helix - The Scientific Explorer, Vol. 9, No. 04, pp. 5122-5127, 2019.